REMARKS

Claims 21-41 were pending and stand rejected, of which claims 21, 28 and 35 are independent. Applicant respectfully notes that the claims were incorrectly numbered. In particular, the claims should be numbered 22-42 as oppose to 21-41. However, to reduce the chance of further confusion and error, Applicant maintained the numbering used the office action. Applicant amended claims 21, 28, and 35, and added claims 42 and 43. Claims 21-43 are now pending, of which claims 21, 28, and 35 are independent. Applicant respectfully requests reconsideration in view of the foregoing amendments and following remarks.

Section 102 Rejections

Claim 21 stands rejected under 35 U.S.C. Section 102(a) as being allegedly anticipated by NIST Special Publication 800-19-Mobile Agent Security ("Jansen"). Applicant respectfully traverses the rejection. However, to expedite prosecution, Application amended claim 21. Support for the amendment can be found in the specification at least at page 2, lines 16-20 and at Fig. 7a and the corresponding text. Claim 21 now recites a system that includes "a server, in communication with a first host and a second host, the first and second hosts executing a mobile application that jumps from the first host to the second host during execution and passes through the server." The server stores, "prior to a jump to the second host, a first instance of the mobile application, an instance of the mobile application including executable code for the mobile application." The server receives "from the first host, during the jump to the second host, a second instance of the mobile application." The server detects "unwanted changes in contents of the mobile application including comparing the first and second instances."

The Examiner contends that Jansen discloses the above-cited limitations of claim 21. In particular, the Examiner contends that Jansen, at Figure 1 and page 2, second paragraph, teaches "the server storing, prior to a jump to the second host, a first instance of the mobile application." Applicant must respectfully disagree. The portion of Jansen relied on by the Examiner describes only a simple model for describing an agent system. The model consists "of only two main components: the agent and the agent platform. Here, an agent is comprised of the code and state

information needed to carry out some computation. Mobility allows an agent to move, or hop, among agent platforms. The agent platforms provide the computational environment in which an agent operates. The platform from which the agent originates is referred to as the home platform, and normally is the most trusted environment for an agent. One or more hosts may comprise an agent platform, and an agent platform map support several computational environments, or meeting places, where agents can interact." Page 2, second paragraph. No where in the portion at issue, however, is there any mention of a server. Furthermore, figure 1 simply does not include any server. Indeed, the arrow representing the path of travel of the mobile application in figure 1, i.e., from one platform directly to another platform, indicates that the simple model described is peer-to-peer and not client-server. Thus, the portion at issue not only fails to mention a server, but also teaches away from a client-server model of claim 21 by showing a peer-to-peer model. Moreover, the portion at issue does not disclose or suggest the operation recited as being performed by the server, i.e., storing, prior to a jump to a host, a first instance of the mobile application, as required by claim 21. Accordingly, the second paragraph of page 2 fails to teach "the server storing, prior to a jump to the second host, a first instance of the mobile application," as recited by claim 21.

The Examiner also relies on Section 2.1.2, Section 3.2, page 9, and Section 4.2.2. The applicant respectfully submits that none of these portions teaches "the server receiving from the first host, during the jump to the second host, a second instance of the mobile application" and "the server detecting unwanted changes in contents of the mobile application including comparing the first and second instances." Section 2.1.2 describes a type of threat referred to as a denial of service to an agent platform. "Mobile agents can launch denial of service attacks by consuming an excessive amount of the agent platforms' computing resources . . . . Depending on the level of access, the agent may be able to completely shutdown or terminate the agent platform." Section 2.1.2. No where in the portion at issue, however, is there any mention of a server. Moreover, a description of a denial of service attack, without more, does not teach the operations recited as being performed by claimed server. Specifically, Section 2.1.2 is simply silent on the "server receiving from the first host, during the jump to the second host, a second

instance of the mobile application" and "the server detecting unwanted changes in contents of the mobile application including comparing the first and second instances," as recited by claim 21.

Section 3.2 describes integrity, which is one of four security requirements. *See* page 8, second to last paragraph. Section 3.2. explains that agent platform must protect agents from unauthorized modification of their code, state, and data, and must ensure that only authorized agents or processes carry out any modification of shared data. *See* page 9, last paragraph. The secure operation of the mobile agent depends on the integrity of the local and remote agent platforms. System access controls must be in place. Section 3.2 also describes attacks directed against messages sent intra or inter-platform. *See id.* No where in the portion at issue, however, is there any mention of a server. Moreover, a description of a requirement of integrity, without more, does not teach the operations recited as being performed by the server. Specifically, Section 3.2 is simply silent on the server "receiving from the first host, during the jump to the second host, a second instance of the mobile application" and "the server detecting unwanted changes in contents of the mobile application including comparing the first and second instances," as recited by claim 21.

Page 9 includes most of Section 3.1, which describes confidentiality, which is a second of the four security requirements. Section 3.1 explains that any private data stored on an agent platform or carried by an agent must remain confidential. Eavesdroppers can gather information about an agent's activities not only from the content of messages being exchanged, but also from message flow from one agent to another. Mobile agents, thus, may want to keep their location confidential. Furthermore, audit log content must also be kept confidential. No where in the portion at issue, however, is there any mention of a server. Moreover, a description of a requirement of confidentiality, without more, does not teach the operations recited as being performed by the server, i.e., "the server receiving from the first host, during the jump to the second host, a second instance of the mobile application" and "the server detecting unwanted changes in contents of the mobile application including comparing the first and second instances," as recited by claim 21.

Section 4.2.2 describes mutual itinerary recording, which is a scheme in which an agent records and tracks a peer agent's itinerary and vice versa. When moving between platforms, the agent sends information regarding the last platform, current platform, and next platform to the peer agent. The peer agent takes appropriate action when inconsistencies are detected. The scheme can be implemented for more than two agents. No where in the portion at issue, however, is there any mention of a server. Moreover, a description of a mutual itinerary recording, without more, does not teach the operations recited by claim 21 as being performed by the server. Specifically, Section 4.2.2 simply does not disclose or suggest that mutual itinerary recording includes "receiving from the first host, during the jump to the second host, a second instance of the mobile application," where "*an instance of the mobile application includ[es] executable code for the mobile application*" (emphasis added). Applicant respectfully submits that itineraries are data and, hence, do not constitute executable code for the mobile application, as required by claim 21.

The Examiner appears to contend that page 19, lines 1-3 of Jansen somehow compensates for the above-described missing information. To the extent that the Examiner so contends, Applicant must respectfully disagree for the following reason.

The portion at issue is essentially one statement regarding the Jumping Bean agent system, which is that the system "addresses some security issues by implementing a client-server architecture, whereby an agent always returns to a secure central host first before moving onto any other platform." However, Jansen does NOT further describe the Jumping Bean agent system. Jansen does NOT describe operations that are performed by the central host. Jansen, hence, does not disclose or suggest that the central host is operable to receive "from the first host, during the jump to the second host, a second instance of the mobile application," where "an instance of the mobile application including executable code for the mobile application" and detect "unwanted changes in contents of the mobile application including comparing the first and second instances," as recited by claim 21.

Applicant respectfully submits that, for at least any of the above reasons, claim 21 and claims depending from claim 21 are in condition for allowance.

Applicant amended claim 28, which now recites a method for verifying integrity of a jumping mobile application. The method includes "storing, prior to a jump and at a server, a first instance of a mobile application that jumps from a first host to a second host during execution, an instance of the mobile application including executable code for the mobile application; receiving, during the jump and at the server, a second instance of the mobile application; and detecting unwanted changes in contents of the mobile application including the server comparing the first and second instances." For at least the reasons set forth above, claim 28 and claims depending on claim 28 are in condition for allowance.

Applicant amended claim 35, which now recites a computer program product including program instructions tangibly stored on a computer-readable medium and operable to cause a computer system to perform a method for verifying integrity of a jumping mobile application. The method includes "storing, prior to a jump and at a location other than a first host or a second host, a first instance of a mobile application that jumps from the first host to the second host during execution, an instance of the mobile application including executable code for the mobile application, receiving, during the jump and at the location, a second instance of the mobile application, and detecting unwanted changes in contents of the mobile application including comparing, at the location, the first and second instances." For at least the reasons set forth above, claim 35 and claims depending on claim 35 are in condition for allowance.

New Claims

Applicant added new claims 42 and 43. Support for claim 42 can be found at least at page 14, line 7 through page 16, line 17. Support for claim 43 can be found at least at page 16, line 18 through page 19. Claims 42 and 43 depend from claim 21 and are allowable for at least the reasons that claim 21 is allowable.

Statement of Substance of Interview

Applicant thanks the Examiner for the courtesy of an interview, held on October 12, 2005. Examiner Jenise E. Jackson and Applicant's representative, Tim H. Pham, participated. The participants discussed the claim numbering, claim 21, and Jansen.

Applicant requests that all pending claims be allowed. Please apply the two-month extension of time fee in the amount of $225.00 and any other appropriate charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: October 20, 2005

Tim H. Pham
Reg. No. 48,589

Customer No. 26181
Fish & Richardson P.C.
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

50307783.doc